

RSA NetWitness

Version 11.7

UEBA Configuration Guide



Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

March 2022

Contents

Introduction	4
UEBA Supported Sources by Schema	4
Authentication Schema	4
File Schema:	4
Active Directory Schema	4
Endpoint Process Schema	5
Endpoint Registry Schema	5
Packet Schema	5
UEBA Configuration	6
ueba-server-config script	6
reset-presidio script	7
UEBA Indicator Forwarder	8
Update Data Source Details	8
Add Features for UEBA Packet Schema	9
Add the Hunting Pack:	9
Add JA3 and JA3s:	10
Assign User Access to UEBA	10
Create an Analysts Role	11
Enable User Entity Behavior Analytics Incident Rule	12
Learning Period Per Scale	14
Learning Period Per Scale for 11.5	14
Physical Machine	14
Virtual Machine	15
Learning Period Per Scale for 11.5.1 and later versions	18
Physical Machine	18
Virtual Machine	19
Troubleshooting UEBA Configurations	21
Task Failure Issues in Airflow	21
User Interface Inaccessible	22
Get UEBA Configuration Parameters	23
Check UEBA Progress Status using Airflow:	23
Check if data is received on the UEBA by Kibana:	24
Scaling Limitation Issue	25
UEBA Policy Issue	26
Troubleshoot Using Kibana	26
Troubleshoot Using Airflow	27

Introduction

RSA NetWitness® UEBA configuration is designed for analysts to perform analytics for leveraged data collected from netwitness logs and networks to perform UEBA analytics.

Note: Mixed mode is not supported for UEBA in NetWitness Platform. The NetWitness server, and UEBA must all be installed and configured on the same NetWitness Platform version.

UEBA Supported Sources by Schema

Authentication Schema

- Windows Logon and Authentication Activity in Version 11.2 - Supported Event IDs: 4624, 4625, 4769, 4648 (device.type=winevent_snare|winevent_nic)
- RSA SecurID Token in Version 11.3.1 - device.type = 'rsaacesrv' ec.activity = 'Logon'
- RedHat Linux in Version 11.3.1- device.type = 'rhlinux'
- Windows Remote Management in Version 11.3.2 - Supported Event IDs: 4624,4625,4769,4648 (device.type=windows)
- VPN Logs and in Version 11.5 - event.type = 'vpn' ec.activity = 'logon'
- Azure AD Logs in Version 11.5 - device.type = 'microsoft_azure_signin_events'

Note: Make sure you have configured the Azure Monitor plugin in your deployment. This enables UEBA to run a query for Azure AD log events for monitoring purposes in the correct format. For more information on how to configure the Azure Monitor plugin, see the *Azure Monitor Event Source Configuration Guide*.

File Schema:

- Windows File Servers in Version 11.2 - Supported Event IDs: 4663,4660,4670,5145 (device.type=winevent_snare|winevent_nic)
- device.type=windows in Version 11.3.1

Active Directory Schema

- Windows Active Directory in Version 11.2 - Supported Event IDs: 4741,4742,4733,4734,4740,4794,5376,5377,5136,4764,4743,4739,4727,4728,4754,4756,4757,4758,4720,4722,4723,4724,4725,4726,4738,4767,4717,4729,4730,4731,4732 (device.type=winevent_snare|winevent_nic)
- device.type=windows in Version 11.3.1

Endpoint Process Schema

- Endpoint Process in Version 11.3 - Category = 'Process Event'

Endpoint Registry Schema

- Endpoint Registry in Version 11.3 - Category = 'Registry Event'

Packet Schema

- TLS in Version 11.4 - Service 443 (direction='outbound')

Note: The TLS Packet requires adding the hunting package and enabling the JA3 features as described in [Add required features for UEBA Packets Schema](#).

UEBA Configuration

This topic provides the high-level tasks required to configure UEBA.

IMPORTANT: Changing the UEBA start-date or the UEBA processed schemas requires a re-run of the UEBA system as well as cleanup of the UEBA databases. In order to avoid deleting the information in the UI, you can use the `reset_presidio.py` script as described in [reset-presidio script](#), it will keep the data in the UI (e.g. Alerts, Indicators, Entities and Scores).

Note: Steps 1 to 4 must be executed as root on the UEBA machine.

ueba-server-config script

The `ueba-server-config` script is usually used to configure and run the UEBA component after the deployment. Also, it can be used to update the UEBA configuration during run time.

IMPORTANT: If you change the start-time or the processing schemas, you must re-run UEBA. All script arguments (except the boolean arguments) are mandatory and must be filled.

For more information on the script parameters, see the NetWitness Installation Guide for Version 11.5.

To run the script use the following command `/opt/rsa/saTools/bin/ueba-server-config --help`

Argument	Variable	Description
-u	<user>	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.
-p	<password>	<p>Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password.</p> <pre>!"#\$%&()*+,-.;<=>?@[\\]^_`{ }</pre> <p>If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:</p> <pre>sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '! "UHfz?@ExMn#\$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v</pre>
-h	<host>	IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.
-o	<type>	Data source host type (<code>broker</code> or <code>concentrator</code>).

Argument	Variable	Description
-t	<startTime>	Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, 2018-08-15T00:00:00Z). <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> Note: The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone. </div>
-s	<schemas>	Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS).
-v		verbose mode.
-e	<argument>	Boolean Argument. This enables the UEBA indicator forwarder to Respond. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> Note: If your NetWitness deployment includes an active Respond server, you can transfer NetWitness UEBA indicators to the Respond server and create incidents by enabling the indicator forwarder, from this data. For more information on how to enable the NetWitness UEBA incidents aggregation, see Enable User Entity Behavior Analytics Incident Rule. </div>

Note: The TLS packet requires adding the hunting package and enabling the JA3 features. For more information, see [Add Features for UEBA Packet Schema](#).

reset-presidio script

IMPORTANT: The reset_presidio.py script deletes the UEBA back-end databases and can also delete the front-end database that is present in the UI.

The reset_presidio.py script is used to re-run the UEBA system as well as to update the UEBA start-date and the processing schemas easily without having to provide all the other parameters required by the ueba-server-config script. This script re-runs the UEBA while it deletes the backed data (models, aggregations, etc.). To delete the front-end data (UI entities and alerts, etc.) use the clean option. If you don't specify a date, the script will set the default start date, a 28 days earlier than the current date. RSA recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must verify that the start date is set to no later than 14 days earlier than the current date.

Note: UEBA requires to process 28 days of data before the alerts can be created.

- If you choose a start date that is less than 28 days before the current date, for example 10 days earlier from the current date, you will have to wait for another 18 days from the current date to see alerts in your UEBA system (if created).
- If you choose a start date that is greater than 27 days, it's recommended to delete the front-end database as well (use the -c) to avoid duplicate alerts.

To run the script, load the Airflow virtual environment variables as follows:

```
source /etc/sysconfig/airflow
source $AIRFLOW_VENV/bin/activate
OWB_ALLOW_NON_FIPS=on python
/var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_
workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_presidio.py --help
deactivate
```

Argument	Variable	Description
-h, --help		Script Help
-c, --clean	<argument>	If true, clean any existing data in Elasticsearch DB (as Alerts, Indicators, Entities, etc), all data will be deleted form the UEBA UI
-s	<schema>	Reconfigure the UEBA engine array of schemas (e.g. [AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS])
-d	<date>	Reconfigure the UEBA engine to start from midnight UTC of this date. If not set, by default reset the start date to 27 days before the current system day, at midnight UTC, to avoid duplicate alerts in the UEBA UI, in case you didn't cleaned the elasticsearch data (-c) (e.g. 2010-12-31)

UEBA Indicator Forwarder

Note: The UEBA Indicator Forwarder is supported by the UEBA from version 11.3 and later. If your NetWitness environment includes an active respond server, you can transfer the UEBA indicators to the respond server and to the correlation server in order to create Incidents. For more information, see [Enable User Entity Behavior Analytics Incident Rule](#).

Run the following command to activate the UEBA Indicator Forwarder:

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op": "replace", "path": "/outputForwarding/enableForwarding", "value": true}]}'
```

To deactivate the UEBA indicator forwarder, change the “value”:true at the request body to be “value”:false.

Update Data Source Details

In order to update the details of the data source you must use the ueba-server-config script. For more information, see [ueba-server-config script](#).



The data sources details are:

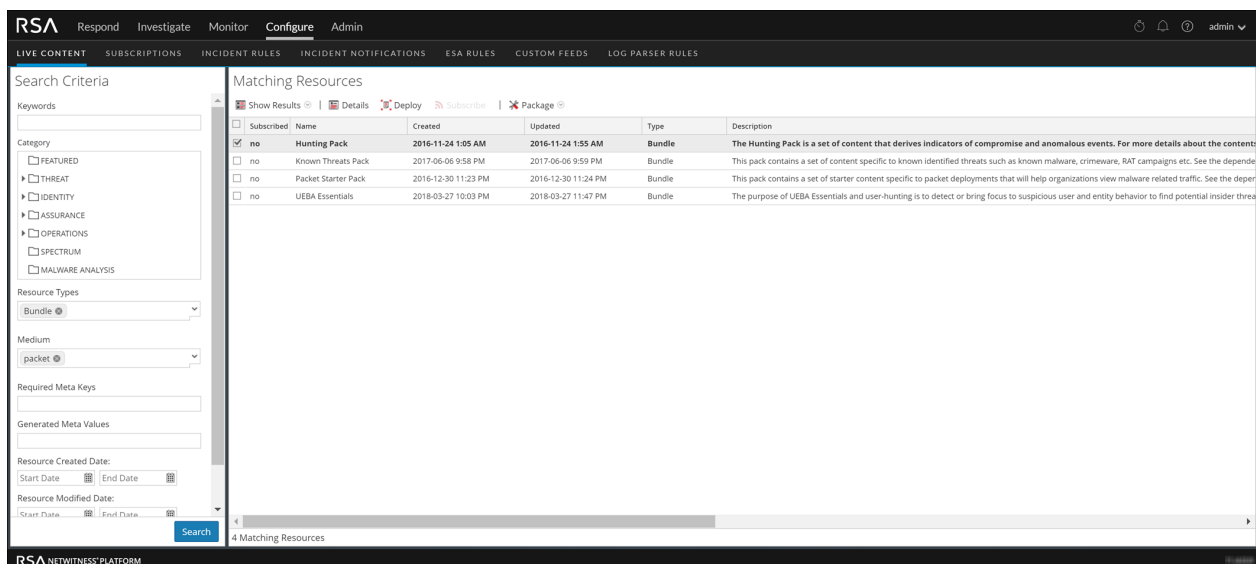
- Data Source type (Broker / Concentrator).
- Data Source username.
- Data Source password.
- Data Source host.

Add Features for UEBA Packet Schema

Add the Hunting Pack:

In NetWitness Platform, add the hunting pack or verify it's available:

1. Login to NetWitness Platform
2. Navigate to  (Admin) and select **Admin Server**
3. Click  and select **Configure > Live Content**



The screenshot shows the RSA NetWitness Platform interface. The top navigation bar includes 'Respond', 'Investigate', 'Monitor', 'Configure', and 'Admin'. The 'Configure' menu is expanded, showing 'LIVE CONTENT', 'SUBSCRIPTIONS', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', and 'LOG PARSER RULES'. The 'LIVE CONTENT' section is active, displaying 'Search Criteria' on the left and 'Matching Resources' on the right. The 'Search Criteria' panel includes fields for 'Keywords', 'Category' (with a tree view showing 'FEATURED', 'THREAT', 'IDENTITY', 'ASSURANCE', 'OPERATIONS', 'SPECTRUM', and 'MALWARE ANALYSIS'), 'Resource Types' (set to 'Bundle'), 'Medium' (set to 'packet'), 'Required Meta Keys', 'Generated Meta Values', and date pickers for 'Resource Created Date' and 'Resource Modified Date'. The 'Matching Resources' table has columns for 'Subscribed', 'Name', 'Created', 'Updated', 'Type', and 'Description'. The table contains four rows, with the first row, 'Hunting Pack', selected. The description for the 'Hunting Pack' reads: 'The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the content...'


Subscribed	Name	Created	Updated	Type	Description
<input checked="" type="checkbox"/>	Hunting Pack	2016-11-24 1:05 AM	2016-11-24 1:55 AM	Bundle	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the content...
<input type="checkbox"/>	Known Threats Pack	2017-06-06 9:58 PM	2017-06-06 9:59 PM	Bundle	This pack contains a set of content specific to known identified threats such as known malware, crimeware, RAT campaigns etc. See the depende...
<input type="checkbox"/>	Packet Starter Pack	2016-12-30 11:23 PM	2016-12-30 11:24 PM	Bundle	This pack contains a set of starter content specific to packet deployments that will help organizations view malware related traffic. See the deper...
<input type="checkbox"/>	UEBA Essentials	2018-03-27 10:03 PM	2018-03-27 11:47 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focus to suspicious user and entity behavior to find potential insider threa...

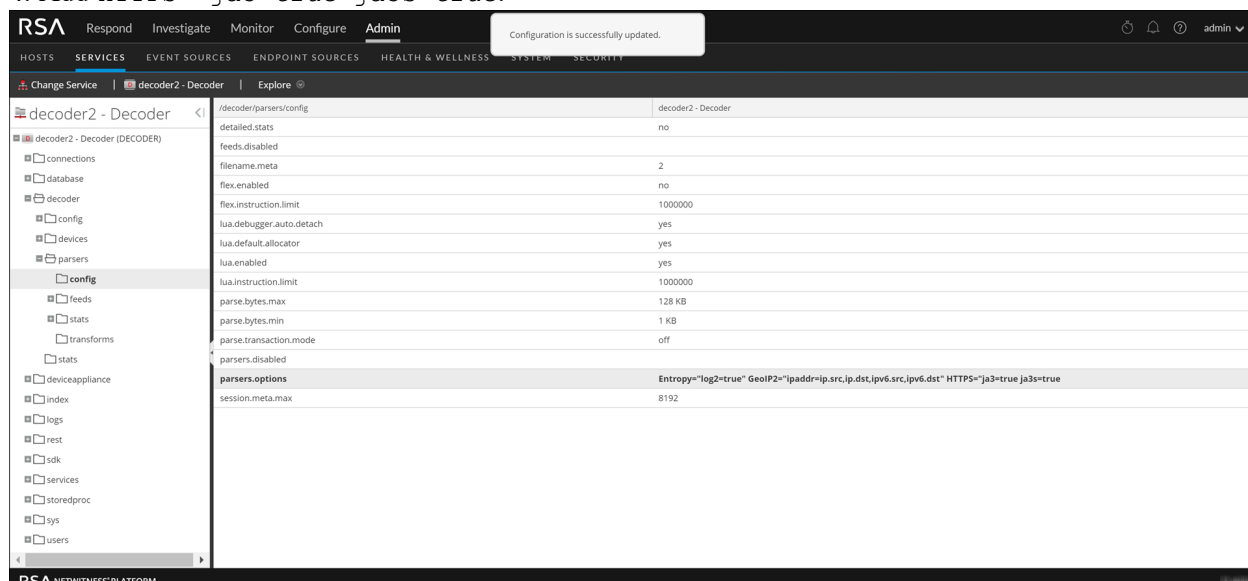
4. On the left menu, select the following:
 - a. Bundle under Resources Type.
 - b. Packet under Medium
5. Click **Search**.
A list of matching resources is displayed.
6. Select **Hunting Pack** from the list and click **Deploy**.
The hunting pack is added.

Add JA3 and JA3s:

The JA3 and JA3s fields are supported by the Network Decoder in 11.3.1 and later. Verify that your Network Decoder is upgraded to one of these versions.

To add JA3 and Ja3s:


1. Log in to NetWitness Platform.
2. Go to  (Admin) and select Decoder.
3. Navigate to `/decoder/parsers/config/parsers.options`.
4. Add `HTTPS="ja3=true ja3s=true`.

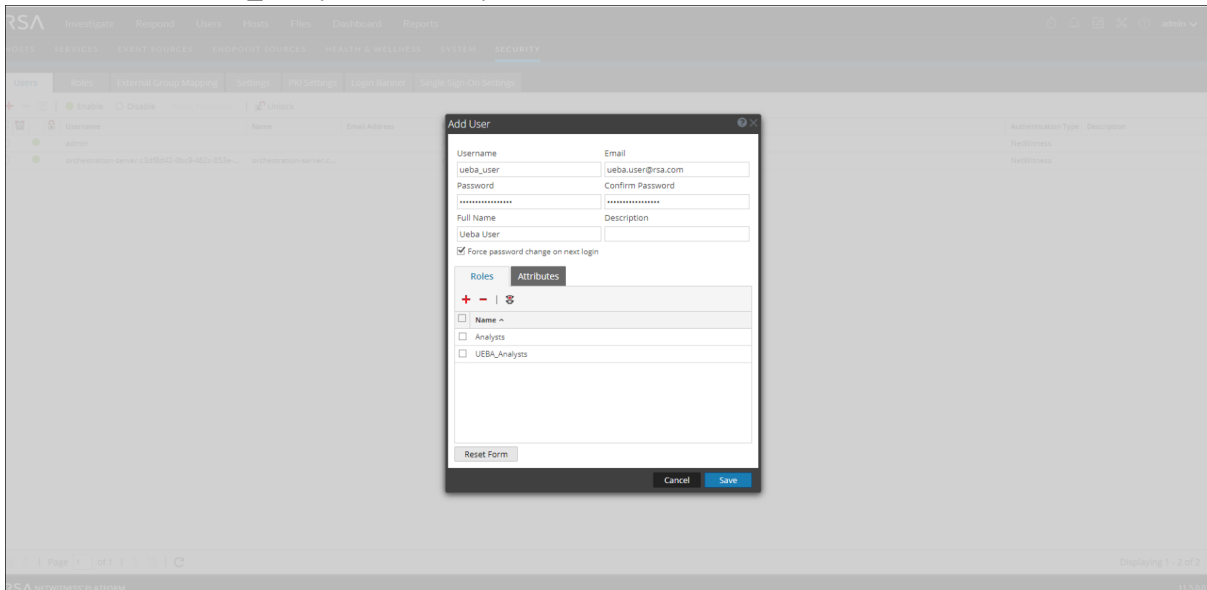


The JA3 and JA3s fields are configured.

Assign User Access to UEBA

To create a user with privileges to access the UEBA pages (Users tab) on the Netwitness UI do the following:


1. Navigate to  (Admin) > **Security**.
2. Create a new UEBA_Analysts and Analysts user roles.



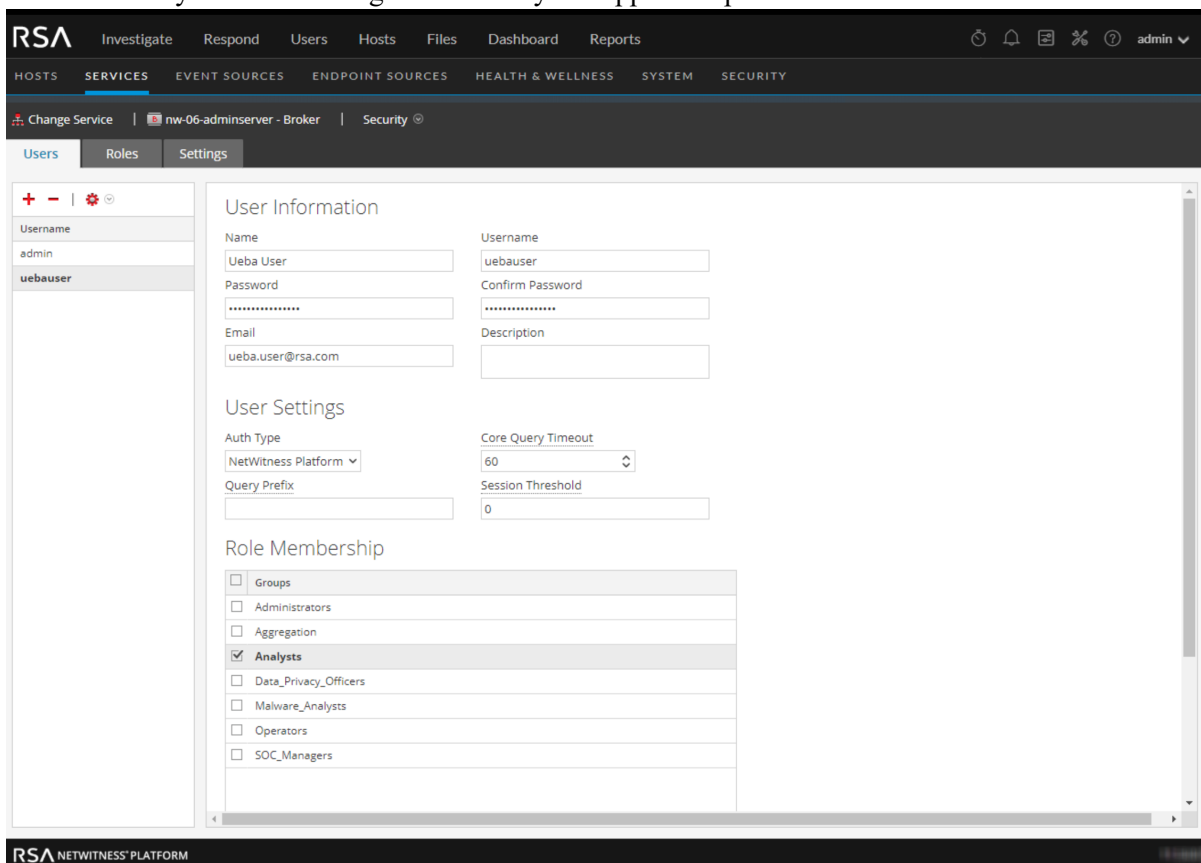
For more information, see the "Manage Users with Roles and Permissions" topic in the *System Security and User Management Guide*.

Create an Analysts Role

In order to fetch data from the data source (Broker / Concentrator), you need to create a user using the "Docktor-UEBA: Validation Too" role in the data source service.

1. Navigate to the security tab at the data source service page.
2.  (Admin) > **Services** > **Security**


3. Create an analyst user and assign it to the any of supported special characters.



Enable User Entity Behavior Analytics Incident Rule

In order to aggregate the UEBA indicators under Incident rule, follow the instructions below:

Enable the UEBA Forwarding process as described in [Enable UEBA Indicator Forwarder](#).

1. Go to  (Configure) > **Incident Rules**.
2. Select the **User Entity Behavior Analytics** rule.
3. Select the enable check box and click **Save**.

The screenshot shows the configuration page for an incident rule in the RSA UEBA system. The interface is dark-themed and includes a top navigation bar with the RSA logo and menu items like 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboards', and 'Reports'. Below the navigation bar, there are tabs for 'LIVE CONTENT', 'SUBSCRIPTIONS', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', 'EVENT RULES', and 'LOG PARSER RULES'. The main configuration area is divided into several sections:

- BASIC SETTINGS:** Includes an 'ENABLED' checkbox, a 'NAME' field with the value 'User Entity Behavior Analytics', and a 'DESCRIPTION' field with the text 'This incident rule captures user entity behavior.'
- MATCH CONDITIONS:** Shows 'QUERY MODE' set to 'Rule Builder'. It features a table of conditions:

FIELD	OPERATOR	VALUE
Source	Is equal to	User Entity Behavior Analytics
UEBA Classifier Id	Is equal to	c0bec74e-880f-42b0-92a1-906c438ab521
- ACTION:** A section titled 'CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT' with two radio buttons: 'Group into an Incident' (selected) and 'Suppress the Alert'.
- GROUPING OPTIONS:** Includes a 'GROUP BY' dropdown set to 'UEBA Classifier Id' and a 'TIME WINDOW' dropdown set to '1 Hours'.
- INCIDENT OPTIONS:** Includes a 'TITLE' field with the template '`\${ruleName} for \${groupByValue}]`' and a 'SUMMARY' field with the placeholder text 'Enter a summary for the incident created by this rule'.

At the bottom right of the configuration area, there are 'Cancel' and 'Save' buttons.

Learning Period Per Scale

Learning Period Per Scale for 11.5

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 20 million network events per day.	Yes	11.5 Installation Up to 4 days with 28 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required.
	Yes	11.5 Upgrade with schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 60 million network events per day.	Yes	11.5 Installation Up to 14 days with 14 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>. </div>
	Yes	11.5 Upgrade with schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>. </div>
Logs and Endpoint data for up to 100,000 users + 60 million network events per day.	No	11.5 Installation 28 days

Virtual Machine

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500MB	500MB

Note: RSA recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends you to deploy UEBA on the physical host as described in the "RSA NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).	Yes	11.5 Installation Up to 4 days with 28 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> UEBA rerun is required.
	Yes	11.5 Upgrade with schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.	Yes	11.5 Installation Up to 14 days with 14 days of historical data.
		11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
		11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="927 1087 1421 1236" style="border: 1px solid green; padding: 5px;"> Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>. </div>
		11.5 Upgrade with schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="927 1444 1421 1593" style="border: 1px solid green; padding: 5px;"> Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>. </div>
Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.	No	11.5 Installation 28 days

Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see [Troubleshooting UEBA Configurations](#).

Learning Period Per Scale for 11.5.1 and later versions

Note: For all supported scales, when historical data is not available, the learning period is 28 days.

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period <small>Alerts will be generated when the learning period is complete</small>
<p>Logs and Endpoint data for 100,000 users + 20 million network events per day.</p>	<p>11.5.1 Installation Up to 4 days with 28 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required

<p>Supported Scale for existing NetWitness customers (historical data is available)</p>	<p>Learning Period Alerts will be generated when the learning period is complete</p>
<p>Logs and Endpoint data for 100,000 users + 60 million network events per day.</p>	<p>11.5.1 Installation Up to 14 days with 14 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="760 764 1419 884" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div> <p>11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="760 1056 1419 1176" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>

Virtual Machine

If there is not historical data, then the learning period will be 28 days.

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500MB	500MB

Note: RSA recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends you to deploy UEBA on the physical host as described in the "RSA NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
<p>Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).</p>	<p>11.5.1 Installation Up to 4 days with 28 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required
<p>Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.</p>	<p>11.5.1 Installation Up to 14 days with 14 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> <p>11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p>
<p>Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see Troubleshooting UEBA Configurations.</p>	

Troubleshooting UEBA Configurations

This section provides information about possible issues when using RSA NetWitness UEBA.


Task Failure Issues in Airflow

Problem	The <code>userId_output_entities</code> task fails when the username contains a backslash.
Cause	When events with usernames containing a backslash character is passed through UEBA, then the <code>userId_output_entities</code> task fails.
Solution	<p>To resolve these issue contact the customer success to obtain the relevant files and execute the following steps:</p> <ul style="list-style-type: none"> • Stop airflow-scheduler service. • Remove all MongoDB documents in the "aggr", "accm" and "input" collections that contains <code>context.userId</code> with hashtag. These documents can be located using the <code>FindCollecionsContainsBackslash.js</code> script. • Replace the <code>/var/netwitness/presidio/flume/conf/adapter/transformers/authentication.json</code> file with the updated authentication .json. • Restart the airflow-scheduler service. • Validate that the next run of the <code>userId_output_entities</code> task is completed successfully.

Problem	The <code>AUTHENTICATION_userId_build_feature_historical_data</code> task fails when the username contains a hashtag.
Cause	When events with usernames containing a hashtag character is passed through UEBA, then the <code>AUTHENTICATION_userId_build_feature_historical_data</code> task fails.
Solution	<p>To resolve these issue contact the customer success to obtain the relevant files and execute the following steps:</p> <ul style="list-style-type: none"> • Stop airflow-scheduler service. • Remove all MongoDB documents in the "aggr", "accm" and "input" collections that contains <code>context.userId</code> with hashtag. These documents can be located using the <code>FindCollecionsContainsHashtagContextUserId.js</code> script. • Replace the <code>/var/netwitness/presidio/flume/conf/adapter/transformers/authentication.json</code> file with the updated authentication .json. • Restart the airflow-scheduler service.

- Validate that the next run of `AUTHENTICATION_userId_build_feature_historical_data` task is completed successfully.

User Interface Inaccessible

Problem	The User Interface is not accessible.
Cause	You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.
Solution	<p>Complete the following steps to remove the extra NetWitness UEBA service.</p> <ol style="list-style-type: none"> 1. SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services. <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre> 2. From the list of services, determine which instance of the <code>presidio-airflow</code> service should be removed (by looking at the host addresses). 3. Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services): <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> <div data-bbox="711 1430 1414 1570" style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: Run the following command to update NW Server to restore NGINX:</p> <pre># orchestration-cli-client --update-admin-node</pre> </div> 4. Log in to NetWitness, go to  (Admin) > Hosts, and remove the extra NetWitness UEBA host.

Get UEBA Configuration Parameters

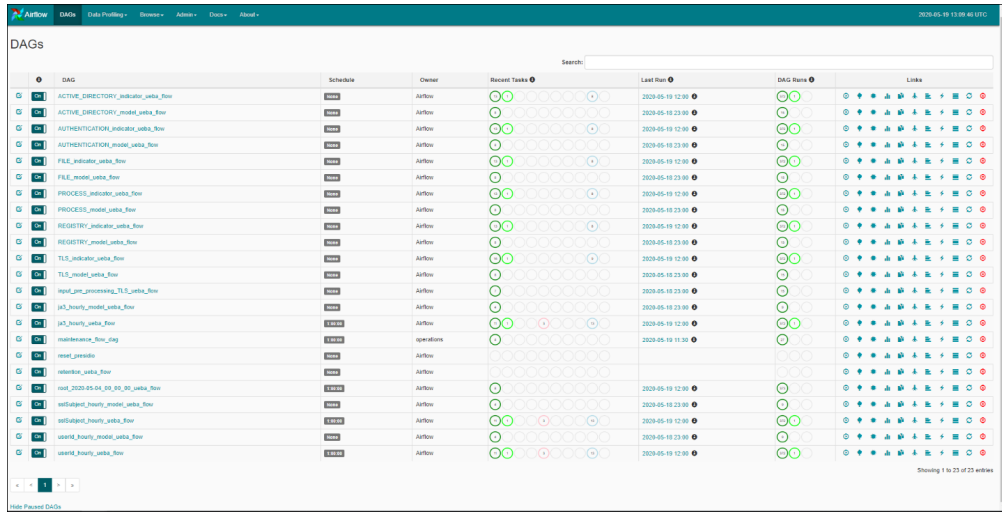
Issue	How to get UEBA configuration parameters?
Explanation	<p>In order to get the UEBA configuration main parameters, run the <code>curl http://localhost:8888/application-default.properties</code> command from the UEBA machine.</p> <pre>[root@UEBA ~]# curl http://localhost:8888/application-default.properties dataPipeline.schemas: AUTHENTICATION,FILE,ACTIVE_DIRECTORY,PROCESS,REGISTRY,TLS dataPipeline.startTime: 2020-11-05T08:00:00Z elasticsearch.clustername: elasticsearch elasticsearch.host: localhost elasticsearch.port: 9200 enable.metrics.export: true entity.batch.size: 1000 entity.score.alert.contribution.critical: 50 entity.score.alert.contribution.high: 10 entity.score.alert.contribution.low: 5 entity.score.alert.contribution.medium: 10 events.store.page.size: 1000 indicators.store.page.size: 1000 mongo.db.name: presidio mongo.db.password: 514p5vIVsCNDkIIlHhbat+dsafdsfdfdsfdfdsafdsfdfdsafdsfdfdsafdsf/X3Y5Sh mongo.db.user: presidio mongo.host.name: localhost mongo.host.port: 27017 mongo.map.dollar.replacement: #dir# mongo.map.dot.replacement: #dot# monitoring.fire.rate: 1000 outputForwarding.enableForwarding: true presidio.execute.ttl.cleanup: false severity.critical: 50 severity.high: 10 severity.mid: 5 spring.autoconfigure.exclude: org.springframework.boot.autoconfigure.data.elasticsearch.ElasticsearchDataAutoConfiguration, org.springframework.boot.autoconfigure.jdbc.DataSourceAutoConfiguration, org.springframework.boot.autoconfigure.integration.IntegrationAutoConfiguration uiIntegration.brokerId: 36973efb-579a-47f3-becc-95a5aa64b34e</pre>
Resolution	<p>The main parameters which will be returned are the following:</p> <ul style="list-style-type: none">• <code>uiIntegration.brokerId</code>: The Service ID of the NW data source (Broker / Concentrator)• <code>dataPipeline.schemas</code>: List of schemas processed by the UEBA• <code>dataPipeline.startTime</code>: The date the UEBA started consuming data from the NW data source• <code>outputForwarding.enableForwarding</code>: The UEBA Forwarder status <p>See the resolution for these statistics in the Troubleshooting UEBA Configurations section.</p>

Check UEBA Progress Status using Airflow:

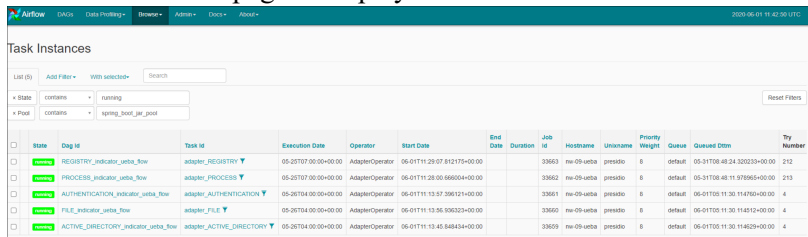
Issue	How to check UEBA progress status using Airflow?
-------	--

Resolution

1. Navigate to- <https://<UEBA-host-name>/admin>. Enter the admin username and the deploy-admin password. The following image is of the Airflow home page that shows the system is working as expected.



2. Make sure that no red or yellow circles appear in the main page:
 - red circle indicates that a task has failed.
 - yellow circle indicates that a task has failed and is “awaiting” for a retry. If a “failed” or “up-for-retry” task appears, investigate what is the root cause of the problem.
3. Make sure the system continues to run.
4. Tap the **Browse** button and select **Task Instance**.
5. Add the following filters: **State** = running and **Pool** = spring_boot_jar_pool. The Task Instance page is displayed.



The **Execution Date** column shows the current time window for each running task. Make sure the execution date is greater than the UEBA start-date and that new tasks have an updated date are added to the table.

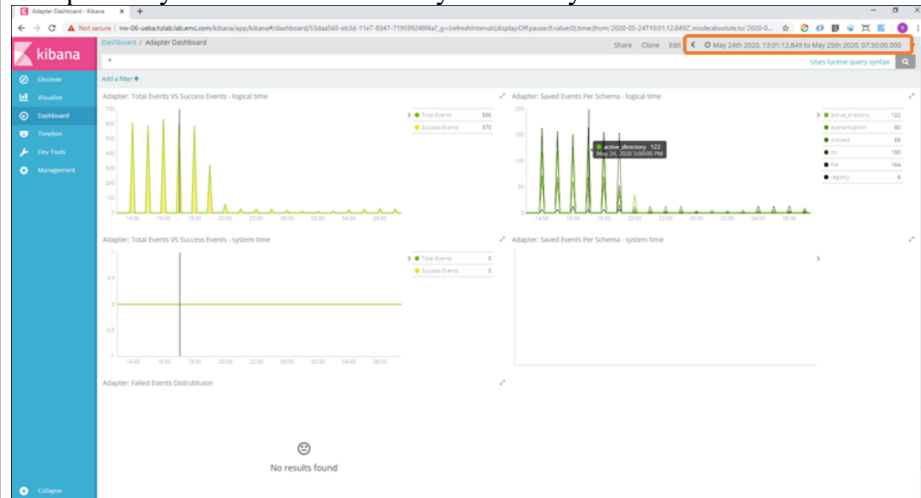
Check if data is received on the UEBA by Kibana:

Issue

How to check if data is received on the UEBA by Kibana:

Explanation

Navigate to- <https://<UEBA-host-name>/kibana>. Enter the admin username and password: To check that the data is flowing to the UEBA go to the Adapter Dashboard: Tap the Dashboard tab in the left menu Tap Adapter Dashboard at the right menu Select the relevant time range at the top bar The charts on this dashboard will present you the data that already fetched by the UEBA.



Scaling Limitation Issue

When installed on a Virtual Machine, UEBA can process up to 20 million network events per day. Based on this limitation, you may encounter the following issues.

Issue	How to determine the scale of network events currently available, to know if it exceeds the UEBA limitation.
Solution	<p>To know the network data limit, perform the following :</p> <ul style="list-style-type: none"> Run the query on the Broker or Concentrator that connects to UEBA using NetWitness UI: <pre>service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443</pre> <p>Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA's supported scale is exceeded.</p>

Issue	Can UEBA for Packets be used if UEBA's supported scale is exceeded?
Solution	<p>You must create or choose a Broker that is connected to a subset of Concentrators that does not exceed the supported limit.</p> <p>To know the network data limit, perform the following :</p> <ul style="list-style-type: none"> Run the query on the Concentrator that connects to UEBA using NetWitness UI:

	<pre>service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443</pre> <p>Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA's supported scale is exceeded.</p>
--	---

Note: The Broker must query all the available and needed data needed such as logs, endpoint and network (packets). UEBA packets models are based on the whole environment. Hence, make sure that the data parsed from the subset of Concentrators is consistent.

UEBA Policy Issue

Issue	After you create a rule under UEBA policy, duplicate values are displayed in the Statistics drop-down.
Solution	<p>To remove the duplicate values, perform the following:</p> <ol style="list-style-type: none"> 1. Log in to MongoDB using following command:<code>mongo admin -u deploy_admin -p {Enter the password}</code> 2. Run the following command on MongoDB: <pre>use sms; db.getCollection('sms_statdefinition').find({componentId : "presidioairflow"}) db.getCollection('sms_statdefinition').deleteMany ({componentId : "presidioairflow"})</pre>

Troubleshoot Using Kibana

Issue	<p>After you deploy NetWitness UEBA, the connection between the NetWitness and NetWitness UEBA is successful but there are very few or no events in the Users > OVERVIEW tab.</p> <ol style="list-style-type: none"> 1. Log in to Kibana. 2. Go to Table of Content > Dashboards > Adapter Dashboard. 3. Adjust the Time Range on the top-right corner of the page and review the following: <ul style="list-style-type: none"> • If the new events are flowing. • In the Saved Events Per Schema graph, see the number of successful events per schema per hour. • In the Total Events vs. Success Events graph, see the total number of events and number of successful events. The number of successful events should be more every hour. <p>For example, in an environment with 1000 users or more, there should be thousands</p>
-------	---

Solution	of authentication and file access events and more than 10 Active Directory events. If there are very few events, there is likely an issue with Windows auditing.
	<p>You must identify the missing events and reconfigure the Windows auditing.</p> <ol style="list-style-type: none"> 1. Go to INVESTIGATE > Navigate. 2. Filter by device.type= device.type “winevent_snare” or “winevent_nic”. 3. Review the events using reference.id meta key to identify the missing events. 4. Reconfigure the Windows auditing. For more information, see NetWitness UEBA Windows Audit Policy topic.

Issue	The historical load is complete and the events are coming from Adapter dashboard but no alerts are displayed in the Users > OVERVIEW tab.
Solution	<ol style="list-style-type: none"> 1. Go to Kibana > Table of content > Scoring and model cache. 2. Adjust the Time Range from the top-right corner of the page, and see if the events are scored.

Issue	The historical load is complete but no alerts are displayed in the Investigate > Users tab.
Solution	<ol style="list-style-type: none"> 1. Go to Kibana > Dashboard > Overview. 2. Adjust the Time Range from the top-right corner of the page, and see how many users are analyzed and if any anomalies are found.

Troubleshoot Using Airflow

Issue	After you start running the UEBA it is not possible to remove a data source during the run process else the process stops.
Solution	You must either continue the process till it completes or remove the required data source from UEBA and rerun the process.

Issue	After you deploy UEBA and if there are no events displayed in the Kibana > Table of content > Adapter dashboard and Airflow has already processed the hours but there are no events. This is due to some communication issue.
Solution	<p>You must check the logs and resolve the issue.</p> <ol style="list-style-type: none"> 1. Log in to Airflow. 2. Go to Admin > REST API Plugin. 3. In the Failed Tasks Logs, click execute.

A zip file is downloaded.

4. Unzip the file and open the log file to view and resolve the error.
5. In the **DAGs > reset_presidio**, click **Trigger Dag**.
This deletes all the data and compute all the alert from the beginning.

Note: During initial installation, if the hours are processed successfully but there are no events, you must click reset_presidio after fixing the data in the Broker. Do not reset if there are alerts.